PROCLAMATION No. …/2021

PROCLAMATION TO PROVIDE FOR PERSONAL DATA PROTECTION

WHEREAS, since to date there is no special law in Ethiopia which governs the rights of individuals on their personal data and the absence of a personal data protection institution has negatively affected the creation of a strong personal data protection system;

WHEREAS, there is a need to establish a personal data protection system in Ethiopia which respects international standards and allows us to maximize the benefits of cross-border transfer of personal data from Ethiopia to outside the country and vice versa;

WHEREAS, there is a need to secure in Ethiopia for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him;

WHEREAS, a personal data protection law is of paramount importance for building an effective digital economy which defines the rights and duties of stakeholders, governs related issues and introduces a system which ensures a strong culture of personal data protection;

NOW, THEREFORE, in accordance with Article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows:

CHAPTER ONE
GENERAL

1. Short Title

This Proclamation may be cited as the Personal Data Protection Proclamation No. …/2021.

2. Definition

In this Proclamation, unless the context requires otherwise,:

(1) "accessible record" means a health record, an education record, or any other accessible public record;

(2) "authorized entity" means a Federal or Regional public body which is delegated by the Commission to perform the powers and functions entrusted to the later by this Proclamation;

(3) "biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person;

(4) "child" means a data subject below the age of sixteen years;

(5) "consent" means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by

(a) a written statement;

(b) verbal affirmations; or

(c) any clear affirmative action

by which he signifies his agreement to personal data relating to him being processed;

(6) "data" means information that:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment mentioned in *lit*. (a),

(c) is recorded as part of a filing system or with the intention that it should form part of a filing system, or

(d) does not fall within *lit*. (a), (b) or (c) but forms part of any other accessible public record;

(7) "data controller" means any person which, alone or jointly with others, has decision-making power with respect to data processing;

(8) "data processor" means any person other than an employee of the data controller who processes the data on behalf of the data controller;

(9) "data subject" means an individual who is the subject of personal data;

(10) "direct marketing" means the communication of any advertising or marketing material which is directed to any particular individuals;

(11) "document" means

(a) a disc, tape or other device in which information other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and

(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

(12) "encryption" means the process of converting data using technical means into coded form;

(13) "filing system" means a structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(14) "genetic data" means personal data relating to the general characteristics of an individual which are inherited or acquired and which provide unique information about the physiology or health of the individual and which result, in particular, from an analysis of a biological sample from the individual in question;

(15) "health record" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his health status;

(16) "identifiable natural person" means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, phone number, IP address, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(17) "personal data" means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(18) "personal data breach" means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(19) "proceedings" means any proceedings conducted by a court or an alternative dispute resolution mechanism; and may include an inquiry or investigation into an offence; and disciplinary proceedings;

(20) "processing" means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(21) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

(22) "pseudonymization" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

(23) "recipient" means any person to whom data are disclosed or made available;

(24) "Register" means the register kept and maintained by the Commission;

(25) "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

(26) "sensitive personal data" means data on a natural person's:

- (a) racial or ethnic origins;
- (b) genetic or biometric data;
- (c) physical or mental health or condition;
- (d) sexual life;
- (e) political opinions;
- (f) membership of a trade union;
- (g) religious beliefs or other beliefs of a similar nature;

(h) the commission or alleged commission of an offence;
(i) any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in the proceedings;
(j) communications data, including content and metadata; or
(k) any other personal data as the Commission may determine to be sensitive personal data.

(27) "third party" means person other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorized to process personal data;

(28) "third party jurisdiction" means a country other than Ethiopia, and an international organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

(29) "traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

(30) "Commission" means the Ethiopian Personal Data Protection Commission;

(31) "House" means the House of Peoples' Representative of the Federal Democratic Republic of Ethiopia;

(32) "person" means a physical or legal person; and

(33) Any expression in the masculine gender shall include the feminine.

3. <u>Scope of Application</u>

(1) This Proclamation shall apply to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data form part of a filing system or are intended to form part of a filing system.

(2) Except as otherwise provided, this Proclamation applies to a data controller or data processor in respect of any personal data only if:
(a) it is established in Ethiopia and the data are processed in the context of that establishment, or
(b) It is not established in Ethiopia, but uses equipment in Ethiopia for processing the data otherwise than for the purposes of transit through Ethiopia and has a representative established in Ethiopia.

(3) For the purpose of the application of sub-Article (2) *lit*. (a) of this Article, this Proclamation shall apply to private and public institutions of the federal and regional governments, including the city administrations of Addis Abeba and Dire Dawa, which have the power and function to process personal data.

(4) Notwithstanding the provisions of sub-Article (1) to (3) of this Article, this Proclamation shall not apply to processing of personal data:
(a) by an individual in the course of purely personal or household activity;
(b) which involves the exchange of information between government agencies where such exchange is required on a need-to-know basis;

(c) exempted under the chapter on exemption; and
(d) which originates outside of Ethiopia and merely transits through this country.

CHAPTER TWO
THE DATA PROTECTION COMMISSION OF ETHIOPIA

4. Establishment

(1) The Data Protection Commission of Ethiopia (hereafter referred as Commission) is hereby established as an independent entity.
(2) The Commission is accountable to the House of Peoples' Representatives.

5. Powers and Functions of the Commission

The Commission shall have the powers and functions to:
(1) ensure compliance with this Proclamation;
(2) make the administrative arrangement it considers appropriate for the discharge of its duties;
(3) levy fees for the services it provides in accordance with a regulation to be issued to implement this Proclamation;
(4) promote public awareness on issues which fall under this Proclamation;
(5) ensure that personal data processed by data controllers and data processors are done according to the data protection principles;
(6) monitor the use of personal data and sensitive personal data; submit periodical reports to the House; and make such documents available to the public;
(7) undertake research into, and monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons are minimized, and report to the House the results of such research and monitoring;
(8) by undertaking researches on the interaction of technology and the right to privacy, performs knowledge creation and capacity building works;
(9) To represent Ethiopia, in coordination with the competent Government body, in international conferences and international organizations concerned with personal data protection; follows up its execution;
(10) cooperate with supervisory authorities of other countries;
(11) make determination as to whether a third party jurisdiction ensures an appropriate level of protection comparable with the level of protection established as per this Proclamation and laws issued to implement this Proclamation;
(12) investigate following legally established investigation procedures and principles complaints made to it, and require information which are relevant for its investigation which will enable it to take administrative measures;
(13) keep and maintain Register of data controllers and data processors;

(14) get injunction order for the expeditious preservation of personal data, including traffic data, where it has reasonable ground to believe that the data are vulnerable to loss or modification;
(15) issue enforcement notice to a data controller or data processor, when it is of the opinion that such bodies have contravened, are contravening or are about to contravene this Proclamation;
(16) impose administrative fines for failures to comply with this Proclamation;
(17) delegate whenever necessary any power conferred on it by this Proclamation to any public entity of the Federal or State Government; and
(18) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commission by or under this Proclamation or any other law or as necessary for the promotion of object of the Proclamation.

6. Organization of the Commission

The Commission shall have:
(1) a Commissioner;
(2) Deputy Commissioners; and
(3) the necessary staff.

7. Head Quarters

The Commission shall have its headquarters in Addis Ababa and may have branch offices at any place within Ethiopia.

8. Budget

The budget of the Commission shall be allocated by the House; and, whenever necessary, may receive financial support from local, foreign and international institutions.

9. Books of Account

(1) The Commission shall keep complete and accurate books of account.
(2) The Commission's books of account and any other financial documents shall be inspected every year by the Auditor General or by an auditor who is assigned by the Auditor General.

10. Appointment and Criteria for Appointment

(1) The Prime Minister shall establish an independent committee which constitutes five members and that will engage in the recruitment of nominees to the position of Commissioner and Deputy Commissioners.
(2) The committee shall:
    (a) receive nominations from the public;
    (b) conduct a transparent and competitive selection process;
    (c) make a short list of five nominees; and
    (d) send the short list to the Prime Minister.

(3) The Prime Minister after receiving the short list of nominees shall select his nominee and communicate the same to the House.

(4) A nominee shall be appointed upon receipt of the support by a two third majority of the House.

(5) The Commissioner and the Deputy Commissioners shall hold office for a term of five and four years respectively, and shall be eligible for a re-appointment only once.

(6) Any person who:
   (a) is loyal to the Constitution of the Federal Democratic Republic of Ethiopia;
   (b) upholds the respect for human rights;
   (c) is trained in law, data science, information technology or other relevant discipline or has acquired extensive knowledge through experience;
   (d) is reputed for his diligence, honesty and good conduct;
   (e) has not been convicted for a criminal offence;
   (f) is an Ethiopian national; and
   (g) is of good health to assume the post

   may be appointed to the position.

11. <u>Grounds and Procedures for Removal of an Appointee</u>

(1) An appointee shall be removed from office or discharged from his responsibility upon the following circumstances:
   (a) upon resignation subject to a prior written notice;
   (b) where it is ascertained that he is incapable of properly discharging his duties due to illness;
   (c) where he is convicted of a serious crime;
   (d) where it is ascertained that he is of manifest incompetence; or
   (e) upon termination of his term of office.

(2) Within six months of the removal or discharge of an appointee, as under sub-Article (1), another appointee shall be made to replace him.

(3) An appointee shall be removed from office, upon the grounds specified under sub-Article (1) *lit*. (b)-(d) of this Article, subsequent to investigation of the matter by a Special Inquiry Committee to be formed by the House.

(4) For the purpose of sub-Article (3) of this Article, an appointee shall be removed from office, where the House finds that the recommendation submitted to it, as supported by the majority vote of the Special Inquiry Committee, is upheld by a two-thirds majority vote.

(5) Upon leaving his position, the Commissioner and the Deputy Commissioners shall not be allowed to work for a private entity that is involved with data controlling or processing.

12. <u>Powers and Functions of the Commissioner</u>

(1) The Commissioner shall be the chief executive of the commission and, as such, shall lead and manage the works of the Commission.

(2) Without prejudice to the generalities of sub-Article (1) of this Article, the Commissioner shall:
   (a) exercise the powers and functions of the Commission specified under Article 5 of this Proclamation;
   (b) prepare the annual work plan and budget of the Commission, and utilize same when approved;
   (c) effect expenditures in accordance with the approved work budget and plan of the Commission;
   (d) represent the Commission in all dealings with third parties;
   (e) prepare the activity and financial reports of the Commission; and
   (f) organize the Commission, and hire and administer employees of the Commission in accordance with civil servants laws.

13. Powers and Functions of the Deputy Commissioners

The Deputy Commissioners shall have the following duties:
(1) perform the activities assigned to them by the Commissioner;
(2) the deputy commissioner delegated by the Commissioner performs the activities of the Commissioner in his absence.

14. Oath and Confidentiality

(1) The Commissioner and Deputy Commissioners shall take an oath at the time of their appointment.
(2) A person who is or has been a Commissioner, a Deputy Commissioner, a member of Commission's staff or an agent of the Commission shall not make use of or divulge, either directly or indirectly, any data obtained as a result of the exercise of a power or in the performance of a duty under this Proclamation, except:
   (a) in accordance with this or any other Proclamation; or
   (b) as authorized by the order of a Court

CHAPTER THREE
PROCESSING OF PERSONAL DATA

15. The Principle of Lawfulness

(1) Personal data shall be processed lawfully.
(2) Notwithstanding the provision of sub-Article (1) of this Article, personal data shall not be processed unless there is compliance with at least one of the conditions set out in sub-Articles (3) and (4) of this Article; or in the case of sensitive personal data, Article 17 of this Proclamation.
(3) The processing of personal data shall meet the following conditions:
   (a) The data subject has given his consent;
   (b) Processing is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering

into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the data controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to a public health crisis or national emergency or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate within the limits of a law issued for this purpose; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal data controller to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection of personal data.

(4) For the purpose of sub-Article (3) *lit*. (e) of this Article,

(a) The law shall pursue public interest objectives;

(b) The interference with privacy through data processing shall be necessary and proportionate;

(c) The law shall determine the essential elements of processing such as the categories of data, the purpose, storage period, and possible disclosure; and

(d) Further processing of personal data after the expiry of such law shall be prohibited.

(5) Data processing shall be proportionate in relation to the legitimate purpose pursued.

16. <u>Conditions for Consent</u>

(1) For the purpose of Article 15 sub-Article (3) *lit*. (a) of this Proclamation, personal data may be processed on the basis of the consent of the data subject, shall be given prior to the commencement of the processing.

(2) For the consent of the data subject to be valid, it must be free, informed, specific, clear and require an active action from the data subject. Where consent has been given verbally, the burden of proof shall rest upon the data controller.

(3) The data subject may withdraw his consent at any time. Information with regard to withdrawal of consent shall be given prior to giving his consent.

(4) The data controller shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose. The application of this provision shall be decided on a case by case basis.

(5) The data controller shall bear the burden of proof to establish that consent has been given by the data subject for processing of personal data in accordance with sub-Article (2) of this Article. The request for consent shall be presented in a manner which is clearly distinguishable and separate from other matters; request for consent cannot be bundled with other terms and conditions.

(6) Where the data subject withdraws consent for the processing of any personal data necessary for the performance of a contract to which he is a party, reasonable legal consequences for the effects of such withdrawal shall be borne by him. The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal.

17. Processing of Sensitive Personal Data

(1) The processing of sensitive personal data shall be prohibited.

(2) Notwithstanding the provision of sub-Article (1) of this Article, the processing of sensitive personal data shall be permitted in the following cases:

(a) The data subject has given his written consent, specific to the purpose prior to the processing except where a law provides that the prohibition referred in sub-Article (1) of this Article may not be lifted by the data subject;

(b) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his consent prior to the processing;

(c) The processing is necessary to achieve the lawful and non-commercial objectives of public organizations;

(d) The processing is necessary for purposes of medical treatment and is carried out by a medical treatment institution;

(e) The processing concerns such personal data as is necessary for the protection of lawful rights and interests of persons in court proceedings, or other public institutions, or

(f) processing is carried out in the course of its legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(3) Sensitive personal data in respect of race or ethnic origin shall not be processed unless the processing is:

(a) for ensuring justice and equality with regard to race or ethnic origin; and

(b) carried out with appropriate safeguards for the rights and freedoms of the data subject.

(4) For the purpose of sub-Article (2) and (3) of this Article, processing shall be permitted if it is done with appropriate safeguards.

18. Further Categories of Sensitive Personal Data

(1) The Commission may by a directive prescribe further categories of personal data which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under sub-Article (1) of this Article, the Commission may specify any further grounds on which such specified categories may be processed, having regard to**:**
   (a) the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;
   (b) the expectation of confidentiality attached to such category of personal data;
   (c) whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and
   (d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Commission may specify other categories of personal data which require additional safeguards or restrictions.

19. <u>Processing of Personal Data of a Child</u>

(1) Data of a child shall be processed in a manner that protects and advances the rights and best interests of the child. The data controller shall bear the burden of proof.

(2) The processing of a child's personal data shall be lawful where and to the extent that:
   (a) consent is given or authorized by the parent or guardian or tutor of the child; or
   (b) processing is necessary to the child's vitally important interest.

(3) The data controller shall make reasonable efforts to verify the age of the data subject and that consent is given or authorized by the parent or guardian of a child, taking into consideration available technology.

(4) Notwithstanding the provisions of sub-Article (1) – (3) of this Article, the processing of personal data of a child for the purposes of marketing, profiling, or merging of profiles shall not be allowed.

20. <u>The Principle of Fairness and Transparency</u>

(1) Personal data shall be processed fairly and in a transparent manner.

(2) For the purpose of sub-Article (1) of this Article, the processing of personal data shall meet the following conditions:
   (a) The data controller or data processor shall take appropriate measures to provide any information relating to processing to the data subject;
   (b) The information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
   (c) Processing shall not be done in a way that is unexpected or misleading to the data subject; or
   (d) Processing shall respect the right to be informed and be done in a manner which is clear, open and honest.

(3) Any information addressed specifically to a child as per the provisions of sub-Article (2) *lit*. (b) of this Article shall be given special attention.

(4) The data controller shall be under a duty to always provide the information stipulated in Article 34 of this Proclamation.

21. The Principle of Purpose Limitation

(1) Personal data shall be obtained only for one or more explicit, specified and lawful purposes.

(2) Personal data shall not be further processed in any manner incompatible with that purpose or those purposes.

(3) For the purposes of the application of the principles stipulated in sub-Articles (1) and (2) of this Article, the purpose for which personal data are obtained shall be specified

(a) in a notice given by the data controller to the data subject prior to that further processing; or

(b) in a description given to the Commission under Article 44 sub-Article (3) *lit*. (e) of this Proclamation.

(4) In determining whether any disclosure of personal data is compatible with the purpose for which the data were obtained, regard is to be had to the:

(a) purpose for which the personal data are intended to be processed by any person to whom they are disclosed; and

(b) functions or activities of the person processing the personal data.

(5) For the purpose of sub-Article (4) of this Article, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes.

22. The Principle of Data Minimization

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

23. The Principle of Accuracy

(1) Personal data shall be accurate and, where necessary, kept up-to-date.

(2) The principle of accuracy is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where:

(a) having regard to the purpose for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and

(b) if the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicates that fact.

24. The Principle of Storage Limitation

(1) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(2) Sub-Article (1) of this Article does not apply to personal data if:

(a) the retention of the record is required or authorized by this or other Proclamations; or

(b) the retention of the record is reasonably necessary for a lawful purpose related to a function or activity.

(3) Sub-Article (1) of this Article does not apply to records of personal data retained for historical, statistical, or research purposes.

(5) A person who retains records for historical, statistical or research purposes shall ensure that the records that contain the personal data are adequately protected against access or use for unauthorized purposes.

(6) A person who uses a record of the personal data of a data subject to make a decision about the data subject shall retain the record for a period required or prescribed by law or a code of conduct.

25. <u>The Principle of Integrity and Confidentiality</u>

(1) The data controller shall take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall in order to comply with this principle:

(a) choose a data processor who provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and

(b) take reasonable steps to ensure compliance with those measures.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with this principle unless:

(a) the processing is carried out under a contract which is made or evidenced in writing;

(b) the data processor is to act only on instructions from the data controller; and

(c) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the principle of integrity and confidentiality.

(4) The data controller and data processor shall take technical steps to ensure that any individual acting under their authority and has access to personal data does not process the personal data except on instructions from the data controller, unless he is required to do so by a law.

26. <u>The Principle of Security</u>

(1) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

(2) For the purposes of the application of the principle of integrity and confidentiality regard shall be made to the state of technological development.

(3) The measures referred in sub-Article (2) of this Article must ensure a level of security appropriate to

(a) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage; and

(b) the nature of the data to be protected.

(4) Taking into account the state of the art, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the data controller and the data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:
   (a) the pseudonymization and encryption of personal data;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(5) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing.

(6) For the purpose of sub-Article (5) of this Article, risks shall include in particular those risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

27. <u>The Principle of Data Transfer</u>

Without prejudice to the provisions on data transfer, the transfer to a third party jurisdiction of personal data that is to undergo processing may only take place subject to the provisions of this Proclamation and provided that the third party jurisdiction to which the data is to be transferred ensures appropriate levels of protection.

28. <u>Level of Protection in Third Party Jurisdiction</u>

(1) The appropriate level of protection stipulated under Article 27 of this Proclamation shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations before the data is transferred.

(2) For the purpose of sub-Article (1) of this Article, particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law in force in the third party jurisdiction and the professional rules and security measures which are complied within that jurisdiction.

(3) Where, despite the absence of appropriate levels of protection, the Commission determines that some limited form of transfer may be facilitated which would limit the breach of the data subject's rights in accordance with this Proclamation, the Commission may authorize such a transfer where:
   (a) the data subject consents to the transfer of the data to the third party jurisdiction; and
   (b) there is appropriate severance or reduction of those aspects of the data which the Commission deems appropriate.

(4) Notwithstanding the provision of sub-Article (3) and (4) of this Article, the transfer of personal data to a third party jurisdiction that does not ensure appropriate level of protection is prohibited.

29. Conditions for Cross Border Transfer

(1) A data controller or data processor may transfer personal data to a third party jurisdiction where:
   (a) he has given proof to the Commission on the existence of appropriate level of protection in that third party jurisdiction, and the Commission has made the determination according to sub-Article (3) of Article 28 of this Proclamation;
   (b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate level of protection;
   (c) the transfer is necessary; or
   (d) the transfer is made from a register which, according to law, is intended to provide information to the public.

(2) For the purpose of sub-Article (1) *lit*. (c) of this Article, the transfer is necessary where:
   (a) the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
   (b) for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another person;
   (c) for important reasons of public interest;
   (d) for the establishment, exercise or defence of a legal claim; or
   (e) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

30. Safeguards Prior to Cross Border Transfer

(1) The Commission may request a person who transfers data to a third party jurisdiction to demonstrate the effectiveness of the security safeguards and the existence of compelling legitimate interests.

(2) The Commission may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

31. The Principle of Data Sovereignty

(1) Every data controller or data processor shall ensure the storage, on a server or data center located in Ethiopia, of personal data collected or obtained locally.

(2) The Commission shall prescribe, based on grounds of strategic interests of the state, categories of personal data as critical personal data that shall only be processed in a server or data center located in Ethiopia.

(3) Cross-border transfer of sensitive personal data shall require the prior approval of the Commission.

32. The Principle of Accountability

(1) The data controller and, where applicable, the data processor, shall be responsible for complying with all obligations set out in this Proclamation in respect of any processing undertaken by him or on his behalf.

(2) The data controller shall be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Proclamation.

CHAPTER FOUR
RIGHTS OF DATA SUBJECTS

33. Duration of Personal Data Protection

(1) Privacy rights survive the death of the data subject.

(2) For the execution of the provision of sub-Articles (1) of this Article, privacy rights shall remain valid for ten years after the death of the data subject.

(3) The lawful heir of the data subject may invoke the rights of the data subject at any time within the ten years which follow the death of the data subject.

(4) The consent of the lawful heir is not required if the processed personal data only contain the data subject's name, sex, date of birth and death, the fact of death, and the time and place of burial.

34. Right to be Informed

(1) Where personal data relating to a data subject are collected either from the data subject or other sources, the data subject shall have the right to be provided by the data controller with the following information:

(a) the name and contact details of the data controller;
(b) the name and contact details of the representative of the data controller;
(c) the contact details of the data protection officer of the data controller and his representative;
(d) the purposes of the processing;
(e) whether providing answers to questions are voluntary or compulsory and the possible consequences of failure to reply;
(f) the lawful basis for the processing;
(g) the recipients or categories of recipients of the personal data;
(h) the details of transfers of the personal data to a third party jurisdiction;
(i) the retention periods for the personal data;
(j) the rights available to data subjects in respect of the processing;
(k) the right to withdraw consent;
(l) the right to lodge a complaint with a supervisory authority;
(m) the details of the existence of an automated decision-making, including profiling;
(n) the categories of personal data processed; and

(o) any necessary additional information in order to ensure fair and transparent processing.

(2) Apart from the information listed under sub-Article (1), where personal data have not been obtained from the data subject, the data controller shall provide the data subject with the following information:
   (a) the categories of personal data obtained; and
   (b) the source of the personal data.

(3) Where personal data relating to a data subject are collected from the data subject, the data controller shall provide the data subject with all of the information listed in sub-Article (1) of this Article, at the time when personal data are obtained.

(4) Where personal data relating to the data subject are not collected from the data subject, the data controller shall provide the data subject the information referred to in sub-Article (1) and (2) of this Article:
   (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
   (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
   (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

(5) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data were collected or obtained, as the case may be, he shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

35. Right of Access

(1) A data subject shall have a right to obtain, on request, at reasonable intervals, free of charge, and without excessive delay:
   (a) confirmation of the processing of personal data relating to him;
   (b) the communication in an intelligible form of the data processed;
   (c) all available information on their origin;
   (d) on the period for which the data will be stored; and
   (e) any other information that the data controller is required to provide in order to ensure the transparency of processing in accordance with Article 34 of this Proclamation.

(2) A data subject shall have the right to obtain the information listed in sub-Article (1) of this Article, based on his preference, in an electronic or hard copy format.

36. Exception to the Right of Access

(1) The data controller may refuse to disclose personal data to the individual to whom the data relates where:
   (a) the disclosure would constitute an unjustified invasion of another individual's personal privacy;

(b) it is data that is subject to legal privilege or obtained in the course of an investigation or legal proceeding;
(c) it is health or medical data where the data controller has a reasonable belief that providing access to the data could harm the health or safety of another person; or
(d) it is evaluative or opinion material compiled solely for the purpose of determining suitability or eligibility for employment, the award of government contracts and other benefits where the disclosure would reveal the identity of a source who furnished data in circumstances where it may reasonably be assumed that the identity of the source would be held in confidence.

(2) The data controller may disregard requests from an individual for access to that individual's personal data where it would unreasonably interfere with the operations of the data controller because of the repetitious and systematic nature of the requests, and the requests are frivolous or vexatious.

(3) With regard to sub-Article (1) *lit*. (b) of this Article denial shall be limited to the extent and for as long as access would pose a risk to an investigation or the proper conduct of a legal proceeding.

(4) The decision to refuse to disclose according to sub-Article (1) and (2) of this Article shall be communicated in a written form and has to give detail reasons for the denial.

37. <u>Right to Rectification</u>

(1) Where a data subject believes that the personal data is inaccurate, incomplete, misleading, not-up-to-date, or is otherwise being processed contrary to the provisions of this Proclamation, the data subject shall have, on request, free of charge and without excessive delay, the right that the data controller corrects the data.

(2) On correcting personal data under this provision, the data controller shall notify any other data controller or any third party to whom that data has been disclosed during the one year period before the correction was requested, of such correction.

(3) Upon being notified under sub-Article (2) of this Article of a correction of personal data, the person shall make the correction on any record of that data in its custody or control.

38. <u>Right to Erasure</u>

(1) A data subject shall have, on request, free of charge and without excessive delay, the right to erasure of personal data where:
(a) the data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
(c) the data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing; or
(d) the personal data have been unlawfully processed.

(2) Where the data controller has made the personal data public, he shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

(3) Sub-Article (1) and (2) of this Article shall not apply where the processing of the personal data is necessary:
   (a) for reasons of public interest in the field of public health;
   (b) for the purpose of historical, statistical or scientific research when there is no recognizable risk of infringement of the rights and fundamental freedoms of data subjects;
   (c) for compliance with a legal obligation to process the personal data to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
   (d) for the establishment, exercise or defense of a legal claim.

39. <u>Right to Object</u>

(1) The data subject shall have the right to object in writing at any time to the processing of personal data concerning him unless the data controller demonstrates in a written format compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defense of a legal claim.
(2) Where personal data are processed for the purpose of direct marketing, the data subject may object to processing of personal data concerning him for such marketing, which includes profiling to the extent that it is related to such direct marketing.
(3) Where a data subject objects to processing of personal data for the purpose of direct marketing, the personal data shall no longer be processed for that purpose.
(4) The rights referred to in sub-Articles (1) and (2) of this Article shall be explicitly brought to the attention of the data subject.

40. <u>Restriction of Processing</u>

(1) A data subject shall have the right to request the restriction of processing of personal data where:
   (a) the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;
   (b) the data controller no longer needs the personal data for the purpose of the processing, but the data subject requires them for the establishment, exercise or defense of a legal claim;
   (c) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
   (d) he has objected to the processing pursuant to Article 39 of this Proclamation pending verification as to whether the legitimate grounds of the controller override those of the data subject.
(2) Where processing of personal data is restricted under sub-Article (1) of this Article,
   (a) the personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the data controller shall inform the data subject before lifting the restriction on processing of the personal data.

41. Automated Individual Decision Making

(1) Every data subject shall have the right
   (a) not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or significantly affects him;
   (b) obtain human intervention on the part of the data controller; and
   (c) express his views.

(2) Sub-Article (1) of this Article shall not apply where the decision is:
   (a) necessary for entering into, or performing, a contract between the data subject and a data controller;
   (b) authorized by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
   (c) based on the data subject's explicit consent.

(3) Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual shall not be based on sensitive personal data.

(4) In the cases referred to in sub-Article (2) of this Article, the data to be provided by the data controller under Article 34 of this Proclamation shall include data as to the existence of processing for a decision of the kind referred to in sub-Article (1) of this Article and the envisaged effects of such decision on the data subject.

(5) In the cases referred to in sub-Article (2) *lit*. (a) or (c) of this Article, the data controller shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

42. Right to Data Portability

(1) A data subject has the right to receive personal data concerning him, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under sub-Article (1) of this Article, to another data controller or data processor without any hindrance.

(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.

(4) The right under this Article shall not apply in circumstances where:
   (a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or
   (b) it may adversely affect the rights and freedoms of others.

(5) A data controller or data processor shall comply with data portability requests, free of charge and without excessive delay.

43. Exercise of Rights

Where the data subject is a child, incapable of exercising the rights as enumerated in this Proclamation, the provisions of the Civil Code on guardian, tutor or legal administrator shall be applicable accordingly.

CHAPTER FIVE
DATA CONTROLLERS AND DATA PROCESSORS

Section One
Registration of Data Controllers and Data Processors

44. Registration

(1) In order to process personal data the data controller or the data processor shall be registered with the Commission.

(2) Where a data controller or data processor intends to process personal data for two or more purposes, the Commission shall make separate entries for each purpose in the Register.

(3) The Commission may determine the requirements for registration by a directive.

45. Power to Refuse Registration

(1) The Commission shall not grant an application for registration under this Proclamation where the particulars provided for inclusion in an entry in the Register are insufficient.

(2) Where the Commission refuses an application for registration as a data controller, the Commission shall inform the applicant in writing within fourteen days of its decision and the reasons for the refusal, and

(3) A refusal of an application for registration is not a bar to re-application.

46. Effects of Registration

(1) The Commission shall enter the application in the Register if it is satisfied that the conditions required for registration are met.

(2) The Commission shall issue a certificate of registration which is valid for a period of two years; the certificate shall be renewed every two years.

(3) The Commission may determine the requirements for certificate of registration by a directive.

47. Duty to Notify Change

(1) Data controllers shall have the duty to notify to the Commission matters relating to changes made to the registrable particulars stipulated under Article 46 of this Proclamation.

(2) On receiving any notification, the Commission shall make such amendments of the relevant entry in the Register as are necessary.

48. Removal from Register

A person who wants the removal of its registration may request the Commission such removal to be effected from the Register.

49. Cancellation of Registration

(1) The Commission has the power to cancel a registration or vary its terms and conditions where

(a) any information given to it by the applicant is false or misleading in any material particular; or

(b) the holder of the registration certificate fails, without lawful excuse, to comply with any requirement of this Proclamation; or any term or condition specified in the certificate.

(2) The Commission shall, before cancelling or varying the terms and conditions of a registration certificate, require, by notice in writing, the holder of the certificate to show cause, within 21 days of the notice, why the registration certificate should not be cancelled or its terms and conditions should not be varied.

50. Access by the Public

(1) The Commission:

(a) shall provide facilities for making the information contained in the Register available for inspection by members of the public at all reasonable hours; and

(b) may provide such other facilities.

(2) The Commission shall supply any member of the public with a duly certified copy in writing of the particulars contained in the Register.

51. Data Protection Officer

(1) A data controller or data processor shall designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where:

(a) the processing is carried out by a public body, except for courts acting in their judicial capacity;

(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

(2) A group of entities may appoint a single data protection officer provided that such officer is easily accessible by each entity.

(3) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organizational structures.

(4) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

(5) A data controller or data processor shall publish the contact details of the data protection officer and communicate them to the Commission.

52. Duties of Data Protection Officer

(1) The responsibility of a data protection officer shall be to:
   (a) advise the data controller or data processor and their employees on data processing requirements provided under this Proclamation or any other law;
   (b) ensure on behalf of the data controller or data processor that this Proclamation is complied with;
   (c) facilitate capacity building of staff involved in data processing operations;
   (d) provide advice on data protection impact assessment; and
   (e) cooperate with the Commission and any other authority on matters relating to data protection.

(2) Notwithstanding the provisions of sub-Article (1) of this Article, a data protection officer may be a staff member of the data controller or data processor and may fulfill other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

Section Two
Obligations on Data Controllers and Data Processors

53. Technical and Organizational Measures

(1) The data controller and data processor shall implement the appropriate technical and organizational measures to ensure that processing is performed in accordance with this Proclamation.

(2) The measures referred to in sub-Article (1) of this Article shall include:
   (a) implementing appropriate data security and organizational measures;
   (b) keeping a record of all processing operations;
   (c) performing a data protection impact assessment;
   (d) complying with the requirements for prior authorization from, or consultation with the Commission; and
   (e) designating a data protection officer.

(3) Every data controller and data processor shall implement such internal policies and mechanisms as may be required to ensure verification of the effectiveness of the measures referred to in this Article.

54. Notification of Personal Data Breach

(1) Where there is a personal data breach, the data controller shall within 72 hours after having become aware of it, notify the personal data breach to the Commission.

(2) Where the notification of the personal data breach to the Commission is not made as per the provision of sub-Article (1) of this Article, the notification shall be accompanied by reasons for the delay.

(3) The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

(4) The notification of the personal data breach to the Commission referred to in sub-Article (1) of this Article shall:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach; and

(d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(6) The data controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in order to facilitate the Commission in its assessment of the data controller's compliance with this provision.

55. <u>Communication of Personal Data Breach to Data Subject</u>

(1) Where a personal data breach has occurred, the controller shall communicate the personal data breach to the data subject within 72 hours after having become aware of it.

(2) The communication to the data subject shall describe in clear language the nature of the personal data breach and set out the information in Article 54 sub-Article (4) *lit*. (b)-(d) of this Proclamation.

(3) The communication of a personal data breach to the data subject shall not be required where:

(a) the data controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorized to access it, such as encryption;

(b) the data controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to in sub-Article (1) of this Article is no longer likely to materialize; or

(c) it would involve disproportionate effort and the data controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

(4) Where the data controller has not already communicated the personal data breach to the data subject, the Commission may require it to do so.

56. Prior Security Check

(1) Where the Commission is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, it may inspect and assess the security measures taken under Article 26 sub-Articles (4), (5) and (6) of this Proclamation prior to the beginning of the processing or transfer.

(2) The Commission may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a data controller or data processor under Article 26 sub-Article (4), (5) and (6) of this Proclamation.

57. Record of Processing Operations

(1) Every data controller and data processor shall maintain, including logging, a record of all processing operations under his responsibility.

(2) The record shall set out:

(a) the name and contact details of the data controller or data processor, and, where applicable, his representative and any data protection officer;

(b) the purpose of the processing;

(c) a description of the categories of data subjects and of personal data;

(d) a description of the categories of recipients to whom personal data have been or will be disclosed, including recipients in other countries;

(e) any transfers of data to another country, and the suitable safeguards;

(f) where possible, the envisaged time limits for the erasure of the different categories of data; and

(g) the description of the mechanisms on data security.

(3) The data controller or data processor shall, on request, make the record available to the Commission.

(4) In case of logging,

(a) Data controllers and data processors shall keep logs of personal data processing activities including reading;

(b) Logs recording reading, disclosure and transmission shall enable to ascertain the reasoning for conduct of the specified activities, the date and time thereof and the information about the person who read, disclosed or transmitted the personal data, and the names of the recipients of such personal data;

(c) Logs may be used for verification of legality of personal data processing activities, internal monitoring, ensuring integrity and security of personal data and for criminal proceedings;

(d) Information on logs shall be made available to the Commission;

(e) The Commission shall establish the retention periods of logs.

58. Data Protection Impact Assessment

(1) Where processing operations may result in a risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes, every data controller or data processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The processing operations referred to in sub-Article (1) of this Article are:
   (a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;
   (b) processing on a large scale of sensitive personal data;
   (c) a systematic monitoring of a publicly accessible area on a large scale; and
   (d) any other processing operations for which consultation with the Commission is required.

(3) An assessment shall include:
   (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;
   (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   (c) an assessment of the risks to the rights and freedoms of data subjects; and
   (d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Proclamation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

(4) Where appropriate, the data controller or data processor shall seek the views of data subjects on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

59. <u>Prior Authorization and Consultation</u>

(1) Every data controller or data processor shall obtain authorization from the Commission prior to processing personal data in order to ensure compliance of the intended processing with this Proclamation and in particular to mitigate the risks involved for the data subjects where a data controller or data processor cannot provide for the appropriate safeguards in relation to the transfer of personal data to a third party jurisdiction.

(2) The data controller or data processor shall consult the Commission prior to processing personal data in order to ensure compliance of the intended processing with this Proclamation and in particular to mitigate the risks involved for the data subjects where:
   (a) a data protection impact assessment indicates that processing operations are by virtue of their nature, scope or purposes, likely to present a high risk; or
   (b) the Commission considers it necessary to carry out a prior consultation on processing operations that are likely to present a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

(3) Where the Commission is of the opinion that the intended processing does not comply with this Proclamation, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.

(4) The Commission shall make public a list of the processing operations which are subject to prior consultation in accordance with sub-Article (2) *lit*. (b) of this Article.

(5) The data controller or data processor shall provide the Commission with the data protection impact assessment and, whenever requested, any other information.

60. <u>Data Protection by Design and by Default</u>

(1) The data controller, where applicable, the data processor shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures designed to:
   (a) implement the personal data processing principles set out in this Proclamation in an effective manner; and
   (b) integrate the necessary safeguards into the processing in order to meet the requirements of this Proclamation and protect the rights of data subjects.

(2) The measures stipulated under sub-Article (1) of this Article shall take into consideration the state of the art, the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

(3) The data controller shall implement the appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing is processed.

(4) Sub-Article (3) of this Article applies to the amount of personal data collected, the extent of processing of the personal data, the period of storage of the personal data and the accessibility to the personal data.

(5) The technical and organizational measures referred to in sub-Article (1) of this Article shall ensure that personal data is not, by default, made accessible without the individual's intervention to an indefinite number of individuals.

61. <u>Duty to Destroy Personal Data</u>

(1) Unless the contrary is stipulated under Article 24 of this Proclamation, where the purpose for storing personal data has lapsed, every data controller shall destroy or delete the personal data as soon as is reasonably practicable.

(2) The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

(3) The data controller shall have the duty to notify any data processor holding the data of its obligation under this Article.

(4) Any data processor who receives a notification under sub-Article (3) of this Article shall, as soon as is reasonably practicable, destroy the data specified by the data controller.

62. <u>Joint Data Controllers</u>

(1) Where two or more data controllers jointly determine the purposes and means of processing of personal data, they shall be joint data controllers.

(2) Joint data controllers shall determine in their contracts their responsibilities, the scope of their obligations and the contact points for data subjects.

CHAPTER SIX
EXEMPTION AND ADMINISTRATION OF JUSTICE

63. General Exemptions

(1) No exception to this Proclamation shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for:

(a) subject to sub-Article (4) of this Article, the protection of national security, defence or public security;

(b) the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;

(c) an objective of general public interest, including an economic or financial interest of the State;

(d) the protection of judicial independence and judicial proceedings; or

(e) the protection of a data subject or the rights and freedoms of others.

(2) The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of this Proclamation where the data protection principles, rights of data subject and obligations put on data controllers and data processors, and the security and organizational measures specified in Article 26 sub-Article (4), (5) and (6) of this Proclamation are implemented to protect the rights and freedoms of data subjects involved.

(3) Personal data shall be exempt from any provision of this Proclamation where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defence or public security.

(4) A certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact.

(5) Notwithstanding what is stipulated under sub-Article (4) and (5) of this Article,

(a) The certificate shall be limited in time, clearly specify the personal data category, the purpose of the processing, the safeguards that are put in place, the identity of the data controllers, data processors and the data subject; and

(b) The decision shall be subject to independent review by the House.

64. Enforcement Order

(1) Where the Commission is of the opinion that a data controller or a data processor has contravened, is contravening or is about to contravene this Proclamation, the

Commission may serve an enforcement order on him requiring him to take such steps within such period as may be specified in the order.

(2) An enforcement order served under sub-Article (1) of this Article shall:
   (a) specify the provision of this Proclamation which has been, is being or is likely to be contravened;
   (b) specify the measures that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise;
   (c) specify a period which shall not be less than 21 days within which those measures shall be implemented; and
   (d) state that a right of appeal is available.

(3) On complying with an enforcement order, the data controller or data processor, as the case may be, shall, within the period set, notify:
   (a) the data subject concerned; and
   (b) where such compliance materially modifies the data concerned, any person to whom the data was disclosed during the period beginning 12 months before the date of the service of the order and ending immediately before compliance,

of any amendment.

(4) Where the Commission considers that any provision of the enforcement order may not be complied with to ensure compliance with this Proclamation, it may vary the order and, where it does so, it shall give written notice to the person on whom the order was served.

(5) The information order shall state that the person to whom the order is addressed has a right of appeal against the requirement specified in the order within the period specified under sub-Article (3) *lit*. (c) of this Article.

65. <u>Power to Obtain Information</u>

(1) The Commission may, by a written information order served on any data controller or data processor, request that person, unless it violates public interest, to furnish to it in writing information in the time specified.

(2) The information requested under sub-Article (1) of this Article shall be produced or given access to the Commission in a form in which it can be taken away, is intelligible and is retrievable.

66. <u>Principles of Imposing Administrative Fines</u>

(1) The Commission shall ensure that the imposition of administrative fines pursuant to this Proclamation is effective, proportional and dissuasive.

(2) While deciding to impose administrative fines, the Commission shall have due regard, *inter alias*, to the following factors, namely
   (a) nature, duration and extent of violation of the provisions of the Proclamation, regulations specified thereunder;
   (b) nature and extent of harm suffered by the data subject;
   (c) intentional or negligent character of the violation;

(d) transparency and accountability measures implemented by the data controller or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;
(e) action taken by the data controller or the data processor, as the case may be, to mitigate the damage suffered by the data subject;
(f) previous history of any, or such, violation by the data controller or the data processor, as the case may be;
(g) whether the arrangement between the data controller and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data controller;
(h) the accrual of undue benefits which can be measured; and
(i) any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

67. Administrative Sanctions

(1) Failure to perform the duties stipulated in this Proclamation, regulations, directives and codes of practices issued to implement this Proclamation shall constitute an administrative offence.
(2) When the offence has been committed
(a) by an institution,
(b) in relation to sensitive data, or
(c) the personal data of a child,
the offence shall be punishable to a fine up to four per cent of its total worldwide turnover of the preceding financial year. The local turnover of the company shall make up part of the worldwide turnover of the company.
(3) The Commission may determine by a directive a list of administrative offences and their corresponding sanctions.

68. Administrative Complaints

(1) Anyone who has a complaint against a decision rendered by a data controller or data processor shall have the right to make an administrative complaint to the Commission within twenty one days of such decision.
(2) The Commission after hearing the complaint shall render its decision in writing within twenty one days.

69. Decisions on Administrative Complaints

(1) The Commission
(a) shall upon receiving the notice of appeal inform the data controller concerned and any other affected person of the notice of appeal.
(b) may dismiss the complaint if it holds that it is not supported by enough evidence.
(c) may, if it deems necessary, authorize a mediator to handle the appeal.

(2) The enquiry by the Commission or a mediator may be conducted in private.
(3) The Commission may determine by a directive the administrative procedure to handle complaints.

70. Burden of Proof

Where the data controller refuses to grant the request of the data subject, the burden of proof that the information lies within one of the specified exemptions of the Proclamation is on a balance of probabilities and lies upon the data controller.

71. Criminal Offences and Sanctions

(1) Failure to perform the duties stipulated in this Proclamation shall constitute an offence.
(2) Notwithstanding the provision of sub-Article (1) of this Article,
   (a) Supply information which is false or misleading;
   (b) Failure to comply with any direction issued by the Commission, including failure to comply with an enforcement order;
   (c) Failure to notify personal data breach or implement technical and organizational measure when breach is committed;
   (d) Failure to respect the right of the data subject;
   (e) Processes personal data in contravention of the provisions of this Proclamation;
   (f) Re-identifies personal data which has been de-identified;
   (g) Process re-identified personal data;
   (h) sells or offers to sell personal data;
   (i) transfer of personal data outside Ethiopia in violation of this Proclamation;

   shall be punishable with simple imprisonment.
(3) Notwithstanding the provision of sub-Article (2) of this Article, if the offence has caused any damage and has as a result become a serious offence shall be punishable with rigorous imprisonment.
(4) Notwithstanding the provisions of sub-Article (3) of this Article, when the offence has been committed by an institution or in relation to sensitive data or the personal data of a child, the offence shall be punishable to a fine up to four per cent of its total worldwide turnover of the preceding financial year. The local turnover of the company shall make up part of the worldwide turnover of the company.
(5) The Commission in order to fulfill the administrative responsibilities accorded to it by virtue of this Proclamation shall coordinate with the police and prosecutor; the details shall be governed in a regulation.

72. Appeals Tribunal and Appeals

(1) This Proclamation hereby establishes an independent Appeals Tribunal.
(2) The Appeals Tribunal shall have the power to hear appeals of decisions rendered by the Commission.
(3) The decision of the Commission may be appealed to the Appeals Tribunal within thirty days of the date the decision was rendered

(4) The decision of the Appeals Tribunal may be appealed on issues of law to the Federal High Court within sixty days of the date the decision was rendered.
(5) Notwithstanding the provision of sub-Article (4) of this Article, if the decision against which an appeal is to be made is rendered by a branch of the Commission, an appeal may be made to a regional High Court.
(6) A decision rendered by the High Court shall be final.
(7) The details of the Appeals Tribunal on its organization, powers and responsibilities shall be governed by a regulation.

CHAPTER SEVEN
MISCELLANEOUS PROVISIONS

73. Duty to Cooperate

Every person shall have the duty to cooperate with the Commission in order for the Commission to meet the objective and purpose of this Proclamation and may discharge the powers and functions entrusted to it.

74. Inapplicable Laws

Any law or practice which is inconsistent with this Proclamation shall not be applicable with respect to matters provided for in this Proclamation.

75. Transitionary Provisions

Personal data and sensitive personal data obtained before the effective date of this Proclamation shall be processed or further processed only in accordance with the provisions of this Proclamation.

76. Power to Issue Regulation and Directive

(1) The House may issue regulations to implement this Proclamation.
(2) The Commission may issue directives to implement this Proclamation.

77. Effective Date

This Proclamation shall enter into force as of the date of its publication in the Federal Negarit Gazeta.

Done at Addis Ababa, this ____ day of ____ , 2021.

Sahlework Zewdie
President
Of the Federal Democratic Republic of Ethiopia